UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/670,242	09/26/2000	Mark M. Ishikawa		4706

7590   10/30/2006

ORRICK, HERRINGTON & SUTCLIFFE, LLP
1020 Marsh Road
Menlo Park, CA 94025

EXAMINER
LANIER, BENJAMIN E

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 10/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/670,242	ISHIKAWA ET AL.
	Examiner	Art Unit
	Benjamin E Lanier	2132

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>09 October 2006</u>.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>83-114</u> is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>83-114</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

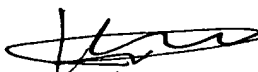8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>23 July 2004</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EУ

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Response to Amendment

1.   The amendment filed 09 October 2006 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: said first unique data identifier being associated with at least one element extraction rule, extracts the first source elements from the source file in accordance with said at least one element extraction rule.

2.   Applicant relies on page 8, line 28 through page 9, line 4, to provide support for the amended claim limitations. While the cited portions of the specification suggest "a set of rules are also defined and associated with the key 30," the cited portions of the specification are completely silent with respect to extracting elements from the data based on the rule, which is associated with a unique identifier. MPEP 2163.05 states that to comply with the written description requirement of 35 U.S.C. 112, paragraph. 1, or to be entitled to an earlier priority date or filing date under 35 U.S.C. 119, 120, or 365(c), each claim limitation must be expressly, implicitly, or inherently supported in the originally filed disclosure. Applicant has failed to show that the limitations are expressly, implicitly, or inherently supported in the originally filed disclosure.

      Applicant is required to cancel the new matter in the reply to this Office Action.

Response to Arguments

3.   Applicant's arguments filed 09 October 2006 have been fully considered but they are not persuasive. Applicant's argue that the specification supports the amendments from 12 August

2005, specifically "said key generation system generates a second unique data identifier for the source file," and the corresponding limitations having specifically to deal with the second unique data identifier. This argument is not persuasive.

4.   MPEP 2163.05 states that to comply with the written description requirement of 35 U.S.C. 112, paragraph. 1, or to be entitled to an earlier priority date or filing date under 35 U.S.C. 119, 120, or 365(c), each claim limitation must be expressly, implicitly, or inherently supported in the originally filed disclosure. Applicant points to page 8, lines 22-23, page 10, lines 14-18, and page 16, lines 20-26, to show support the above mentioned subject matter. These sections of the specification, alone or in combination, fail to disclose the subject matter discussed. The cited section of page 8 talks solely about "defining and generating **a data identifier or key.**" Where **a data identifier** is singular, and not specified as unique. The cited section of page 10 discusses sets of keys and does not refer to unique identifiers for files. The cited section of page 16 recites (from lines 20-21), "Once the data is received from an owner, a **unique identifier**, or source print, is created for the data." Once again, this is only one identifier. Later on page 16 (lines 25-26), the specification recites, "In this manner, **an unlimited number of unique identifiers**, or keys, can be defined for use." This section of the specification does not expressly recite that these unlimited number of unique identifiers are defined for a single file as claimed. This section of the specification does not even recite generation of the unlimited number of unique identifiers, merely defining. Therefore, the specification does not provide support for generating more than one unique data identifier for a single file. Likewise, because the specification fails to support the generation of more than one unique data identifier, all claims limitations that utilize a second identifier are also not support by the specification. Applicant has

failed to show that the limitations are expressly, implicitly, or inherently supported in the

originally filed disclosure.

5.   Applicant argues that Rabin does not teach, "associating a first unique data identifier is

associated with at least one element extraction rule," or "extracting the first source elements

from the source file in accordance with the element extraction rule." This argument is not

persuasive because Rabin discloses that if the supervising program discovers that the software is

untagged, a fingerprint of the software is computing using selected portions of the software and

storing the fingerprint in a fingerprint table of the user device (Col. 20, lines 63-65). A

fingerprint is a unique encoding of one or more portions or data areas selected from an instance

of software (Col. 36, lines 52-54). Including a fingerprint of an instance of software within a tag

associated with that instance permits a supervising program in a user device to verify that the

association between the instance of software and the tag is correct by performing **a same**

location fingerprint check on the instance of software and comparing with the list of fingerprints

in the associated tag (Col. 36, lines 58-65). This shows that the fingerprints are generating using

the same formula or extraction rule, because if you want to compare the fingerprints to determine

if instances of software are the same, you would want to extract the same portions of that

software for comparison. Otherwise, if you extracted different portions for comparison, the

instances of software could be exact copies yet not result in a match upon comparison.

Furthermore, this fingerprint would be associated with the extraction rule used in its creation.

Otherwise, the supervising program would not know which portions of the instance of software

to extract in order to compare the fingerprints as taught in Rabin (Col. 36, lines 61-65).

Claim Objections

6.   Claim 113 is objected to because of the following informalities: "with a plurality data

values" should be changed to "with a plurality of data values." Appropriate correction is

required.

Claim Rejections - 35 USC § 112

7.   The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making
> and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it
> pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode
> contemplated by the inventor of carrying out his invention.

8.   Claims 83, 93, 95, 96, 99-102 are rejected under 35 U.S.C. 112, first paragraph, as failing

to comply with the written description requirement. The claim(s) contains subject matter which

was not described in the specification in such a way as to reasonably convey to one skilled in the

relevant art that the inventor(s), at the time the application was filed, had possession of the

claimed invention. The added material which is not supported by the original disclosure is as

follows: said key generation system generates a second unique data identifier for the source file,

wherein said source print generation system extracts a second predetermined number of second

source elements from the source file in accordance with said second unique data identifier, and

said database system associates said second unique data identifier and the second source

elements with the source file, said source print detection system compares the second source

elements with corresponding target elements in the target file in accordance with said second

unique data identifier and determines whether coincidence exists between the second source

elements in the source file and the target elements in the target file, said preselected coincidence

level differs from said second preselected coincidence level, said first unique data identifier

being associated with at least one element extraction rule (claims 83, 96), extracts the first source

elements from the source file in accordance with said at least one element extraction rule (claims

83, 96).

9.   Applicant relies on page 8, line 28 through page 9, line 4, to provide support for the

amended claim limitations. While the cited portions of the specification suggest "a set of rules

are also defined and associated with the key 30," the cited portions of the specification are

completely silent with respect to extracting elements from the data based on the rule, which is

associated with a unique identifier. MPEP 2163.05 states that to comply with the written

description requirement of 35 U.S.C. 112, paragraph. 1, or to be entitled to an earlier priority

date or filing date under 35 U.S.C. 119, 120, or 365(c), each claim limitation must be expressly,

implicitly, or inherently supported in the originally filed disclosure. Applicant has failed to show

that the limitations are expressly, implicitly, or inherently supported in the originally filed

disclosure.

Claim Rejections - 35 USC § 102

10.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11.   Claims 83-93, 95-99, 101, 103-111 are rejected under 35 U.S.C. 102(e) as being Rabin by

U.S. Patent No. 6,697,948. Referring to claim 83, Rabin discloses an information protection

system wherein copyright protection of vendor created software is provided using detection and

verification programs. The vendor created software is distributed with a supervising program that

detects whether the software contains an appropriate tag (Col. 20, lines 61-63). If the supervising

program discovers that the software is untagged, a fingerprint of the software is computing using

selected portions of the software and storing the fingerprint in a fingerprint table of the user

device (Col. 20, lines 63-65). A guardian center that includes a fingerprint data structure, and

receives all fingerprints from the user devices for each untagged instance of software installed on

user devices (Col. 20, line 65 – Col. 21, line 3), which meets the limitation of a data management

server system that receives a source file for registration and a target file for comparison with the

source file. The fingerprints are generated from selected portions of the software (Col. 20, lines

63-64), which meets the limitation of a key generation system that generates a first unique data

identifier for the source file by identifying a predetermined number of source elements in the

source file as first source elements. The software vendor identifier can be embedded in the

software as a tag (Col. 36, lines 13-16), which meets the limitation of a data embedding system

that embeds an information block into the source file, said information block including

information pertaining to ownership of intellectual property rights. The fingerprint data structure

stored in the guardian center can be stored along with the software in a database (Col. 5, lines 8-

10 & Figure 2 element 300), which meets the limitation of a database system that stores the

source file with the embedded information block, said first unique data identifier, the first source

elements, and ownership information of the source file. A verification program, resident on the

guardian center, compares each fingerprint received from the user device against the fingerprints

in its fingerprint data structure to determine if an untagged instance of software used on a user

device is an infringing instance of software (Col. 21, lines 3-8), which meets the limitation of a

source print detection system that compares the first source elements with corresponding target

elements in the target file in accordance with said first unique data identifier and that determines

whether coincidence exists between the first source elements in the source file and the target

elements in the target file. If the verification program determines that the fingerprints match,

punitive action is performed (Col. 58, lines 7-19). One form of punitive action is the notification

of the software vendor that created the software (Col. 58, lines 20-23), which meets the

limitation of wherein the data management system accesses ownership information to notify an

owner of the source file if a first preselected coincidence level exists between the first source

elements and the target elements. Rabin discloses that if the supervising program discovers that

the software is untagged, a fingerprint of the software is computing using selected portions of the

software and storing the fingerprint in a fingerprint table of the user device (Col. 20, lines 63-

65). A fingerprint is a unique encoding of one or more portions or data areas selected from an

instance of software (Col. 36, lines 52-54). Including a fingerprint of an instance of software

within a tag associated with that instance permits a supervising program in a user device to verify

that the association between the instance of software and the tag is correct by performing **a same**

location fingerprint check on the instance of software and comparing with the list of fingerprints

in the associated tag (Col. 36, lines 58-65). This shows that the fingerprints are generating using

the same formula or extraction rule, because if you want to compare the fingerprints to determine

if instances of software are the same, you would want to extract the same portions of that

software for comparison. Otherwise, if you extracted different portions for comparison, the

instances of software could be exact copies yet not result in a match upon comparison, which

meets the limitation of a source print generation system that applies said first unique data

identifier to the source file and extracts the first source elements from the source file in

accordance with said at least one element extraction rule. Furthermore, this fingerprint would be

associated with the extraction rule used in its creation. Otherwise, the supervising program

would not know which portions of the instance of software to extract in order to compare the

fingerprints as taught in Rabin (Col. 36, lines 61-65), which meets the limitation of said first

unique data identifier being associated with at least one element extraction rule.

Referring to claim 84, Rabin discloses that the fingerprint data structure stored in the

guardian center can be stored along with the software in a database (Col. 5, lines 8-10 & Figure 2

element 300), which meets the limitation of said database system is at least partially incorporated

with said data management server system.

Referring to claim 85, Rabin discloses that the fingerprints are generated from selected

portions of the software (Col. 20, lines 63-64), which meets the limitation of said source print

generation system extracts the first source elements being defined by element characteristics

selected from the group consisting of an element size, an element start position, and an element

initial position relative to said element start position.

Referring to claims 86, 87, Rabin discloses that the embedded tags include user-defined

information (Col. 36, lines 30-32) and that these tags can be digitally signed (Col. 36, lines 2-4 &

Col. 40, lines 43-47), which meets the limitation of said user-defined information is at least

partially encrypted.

Referring to claims 88, 89, Rabin discloses that the embedded tags can include usage

information (Col. 35, lines 14-17), user device id (Col. 36, lines 30-33 & Col. 44, lines 1-8),

software identifier (Col. 37, lines 40-45), which meets the limitations of mandatory compliance

information, authorized user information, a file description, said mandatory compliance

information includes information selected from the group consisting of identification

information, custodial information.

Referring to claim 90, Rabin discloses that the guardian server communicates with

external computers (Figures 1 & 2).

Referring to claim 91, Rabin discloses that the tag server and guardian server may be

bodily incorporated into the software vendor computer system (Col. 27, lines 48-50), which

meets the limitation of the data management system. The software vendor distributes the

software to the user's (Figure 2, elements 111 & 112), which meets the limitation of said data

management server system provides the source file with said embedded information block to

authorize users associated with one or more of the at least one external computer system.

Referring to claim 92, Rabin discloses that the guardian server contains a verification

program that communications with a supervising program on the individual user devices to

locate target files for comparison against the original source files (Col. 20, line 63 – Col. 21, line

8), which meets the limitation of said source print detection system includes a search member

that searches one or more of the at least one external computer system for target files to be

compared with the source files.

Referring to claim 93, Rabin discloses that a second fingerprint is generated from

location specific information within the software (Col. 4, lines 24-44), which meets the limitation

of wherein said key generation system generates a second unique data identifier for the source

file, wherein said source print generation system extracts a second predetermined number of

second source elements from the source file in accordance with said second unique data

identifier, and said database system associates said second unique data identifier and the second

source elements with the source file.

Referring to claim 95, Rabin discloses that the second fingerprint can be compared with

the software, using the location specific information, to see if the second fingerprint is

representative of the same software (Col. 4, lines 24-44), which meets the limitation of said

source print detection system compares the second source elements with corresponding target

elements in the target file in accordance with said second unique data identifier and determines

whether coincidence exists between the second source elements in the source file and the target

elements in the target file.

Referring to claim 96, Rabin discloses an information protection system wherein

copyright protection of vendor created software is provided using detection and verification

programs. The vendor created software is distributed with a supervising program that detects

whether the software contains an appropriate tag (Col. 20, lines 61-63). If the supervising

program discovers that the software is untagged, a fingerprint of the software is computing using

selected portions of the software and storing the fingerprint in a fingerprint table of the user

device (Col. 20, lines 63-65). A guardian center that includes a fingerprint data structure, and

receives all fingerprints from the user devices for each untagged instance of software installed on

user devices (Col. 20, line 65 – Col. 21, line 3), which meets the limitation of receiving a source

file for registration and a target file for comparison with the source file. The fingerprints are

generated from selected portions of the software (Col. 20, lines 63-64), which meets the

generating a first unique data identifier for the source file by identifying a predetermined number

of source elements in the source file as first source elements. The software vendor identifier can

be embedded in the software as a tag (Col. 36, lines 13-16), which meets the limitation of

embedding an information block into the source file, said information block including

information pertaining to ownership of intellectual property rights. The fingerprint data structure

stored in the guardian center can be stored along with the software in a database (Col. 5, lines 8-

10 & Figure 2 element 300), which meets the limitation of storing the source file with the

embedded information block, said first unique data identifier, the first source elements, and

ownership information of the source file. A verification program, resident on the guardian center,

compares each fingerprint received from the user device against the fingerprints in its fingerprint

data structure to determine if an untagged instance of software used on a user device is an

infringing instance of software (Col. 21, lines 3-8), which meets the limitation of comparing the

first source elements with corresponding target elements in the target file in accordance with said

first unique data identifier and determining whether coincidence exists between the first source

elements in the source file and the target elements in the target file. If the verification program

determines that the fingerprints match, punitive action is performed (Col. 58, lines 7-19). One

form of punitive action is the notification of the software vendor that created the software (Col.

58, lines 20-23), which meets the limitation of accessing ownership information to notify an

owner of the source file if a first preselected coincidence level exists between the first source

elements and the target elements. Rabin discloses that if the supervising program discovers that

the software is untagged, a fingerprint of the software is computing using selected portions of the

software and storing the fingerprint in a fingerprint table of the user device (Col. 20, lines 63-

65). A fingerprint is a unique encoding of one or more portions or data areas selected from an

instance of software (Col. 36, lines 52-54). Including a fingerprint of an instance of software

within a tag associated with that instance permits a supervising program in a user device to verify

that the association between the instance of software and the tag is correct by performing **a same**

location fingerprint check on the instance of software and comparing with the list of fingerprints

in the associated tag (Col. 36, lines 58-65). This shows that the fingerprints are generating using

the same formula or extraction rule, because if you want to compare the fingerprints to determine

if instances of software are the same, you would want to extract the same portions of that

software for comparison. Otherwise, if you extracted different portions for comparison, the

instances of software could be exact copies yet not result in a match upon comparison, which

meets the limitation of applying said first unique data identifier to the source file, extracting the

first source elements from the source file in accordance with said at least one element extraction

rule. Furthermore, this fingerprint would be associated with the extraction rule used in its

creation. Otherwise, the supervising program would not know which portions of the instance of

software to extract in order to compare the fingerprints as taught in Rabin (Col. 36, lines 61-65),

which meets the limitation of said first unique data identifier being associated with at least one

element extraction rule.

Referring to claims 97, 98, Rabin discloses that the fingerprints are generated from

selected portions of the software (Col. 20, lines 63-64), which meets the limitation of said

generating said first unique data identifier includes providing at least one data parameter

associated with a selected characteristic of said first unique data identifier and incorporating said

at least one data parameter into said first unique data identifier, said source print generation

system extracts the first source elements being defined by element characteristics selected from

the group consisting of an element size, an element start position, and an element initial position relative to said element start position.

Referring to claim 99, Rabin discloses that a second fingerprint is generated from location specific information within the software (Col. 4, lines 24-44), which meets the limitation of generating a second unique data identifier for the source file by identifying a second predetermined number of second source elements in the source file, extracting the second source elements from the source file in accordance with said second unique data identifier, and storing said second unique data identifier and the second source elements with the source file.

Referring to claim 101, Rabin discloses that the second fingerprint can be compared with the software, using the location specific information, to see if the second fingerprint is representative of the same software (Col. 4, lines 24-44), which meets the limitation of comparing the second source elements with corresponding target elements in the target file in accordance with said second unique data identifier and determining whether coincidence exists between the second source elements in the source file and the target elements in the target file. If the verification program determines that the fingerprints match, punitive action is performed (Col. 58, lines 7-19). One form of punitive action is the notification of the software vendor that created the software (Col. 58, lines 20-23), which meets the limitation of accessing ownership information to notify an owner of the source file if a second preselected coincidence level exists between the second source elements and the target elements.

Referring to claim 103, Rabin discloses that the software can contain hashes (Col. 3, line 66 – Col. 4, line 9), which meets the limitation of the source file having data in a compressed format.

Referring to claim 104, Rabin discloses that the fingerprints are generated from the non-hashed information within the software (Col. 20, lines 63-64), which meets the limitation of extracting the source elements includes expanding the data of the source file.

Referring to claim 105, Rabin discloses generating concatenated information from the software (Col. 12, lines 33-39), which meets the limitation of said extracting the source elements includes forming a concatenated string of the source elements.

Referring to claim 106, Rabin discloses that the fingerprinting procedure can be standardized (Col. 4, lines 24-31), which meets the limitation of normalizing data of the source file and extracting the normalized data form the source file.

Referring to claim 107, Rabin discloses that the embedded tags include user-defined information (Col. 36, lines 30-32) and that these tags can be digitally signed (Col. 36, lines 2-4 & Col. 40, lines 43-47), which meets the limitation of partially encrypting said information block.

Referring to claim 108, Rabin discloses that the guardian server communicates with external computers (Figures 1 & 2).

Referring to claim 109, Rabin discloses that the guardian server contains a verification program that communications with a supervising program on the individual user devices to locate target files for comparison against the original source files (Col. 20, line 63 – Col. 21, line 8), which meets the limitation of searching one or more of the at least external computer system for target files to be compared with the source file.

Referring to claim 110, Rabin discloses that the tag server and guardian server may be bodily incorporated into the software vendor computer system (Col. 27, lines 48-50), which meets the limitation of the data management system. The software vendor distributes the

software to the user's (Figure 2, elements 111 & 112), which meets the limitation of providing

the source file with said embedded information block to authorized users associated with one or

more of the at least one external computer system.

Referring to claim 111, Rabin discloses that fingerprinting involves a mathematical

function for mapping data to smaller data (Col. 30, lines 26-27), which meets the limitation of

said extracting the first source elements comprises extracting the first source elements from the

source file via compression specific element extraction.

Claim Rejections - 35 USC § 103

12.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

13.   The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459

(1966), that are applied for establishing a background for determining obviousness under 35

U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.
2.   Ascertaining the differences between the prior art and the claims at issue.
3.   Resolving the level of ordinary skill in the pertinent art.
4.   Considering objective evidence present in the application indicating obviousness
       or nonobviousness.

14.   Claims 94, 100 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rabin,

U.S. Patent No. 6,697,948. Referring to claims 94, 100, Rabin discloses that the specific

locations that are used to calculate the fingerprints can be changed over time in response to

piracy attacks (Col. 37, lines 11-14), but Rabin does not disclose that these updated fingerprints

are stored as replacements to the original fingerprints. It would have been obvious to one of

ordinary skill in the art at the time the invention was made to have the newly calculated

fingerprints replace the old fingerprints with the guardian center database in order to reduce the

storage of information that is no longer being utilized within the protection system. If these old

fingerprints were no longer being used, it would have been obvious to one of ordinary skill in the

art to replace them with the new fingerprints.

15.   Claims 112-114 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rabin,

U.S. Patent No. 6,697,948, in view of Agrawal, U.S. Patent No. 5,647,058. Referring to claims

112-114, Rabin discloses that the software can be video data (Col. 2, lines 50-52) and that the

fingerprinting involves a mathematical function for mapping data to smaller data (Col. 30, lines

26-27), which meets the limitation of said receiving the source file includes receiving a source

file with a plurality data values, said receiving a source file includes receiving a video source file

with a plurality of red-green-blue (RGB) data values. Rabin does not disclose fingerprinting the

video data by calculating an average value of the RGB data values of portions of the video data.

Agrawal discloses a method of indexing a multi-media database wherein video data is

fingerprinted using the average of RGB color features (Col. 6, lines 28-38), which meets the

limitations of said extracting the first source elements comprises extracting the first source

elements from the source file via non-compression specific extraction, wherein said extracting

the first source elements includes calculating an average value of the data values for each of the

first source elements, wherein said calculating the average value of the data values comprises

calculating an average value of the RGB data values for each of the first source elements. It

would have been obvious to one of ordinary skill in the art at the time the invention was made to

fingerprint the video data of Rabin using the average of the video RGB data values in order to

create indexes for the database that provide similarity characteristics (Agrawal: Col. 2, lines 3-

16) such that efficient searching of the database can be achieved as taught by Agrawal (Agrawal

Col. 2, lines 38-49).

Conclusion

16.   Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

17.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805.

The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin E. Lanier

KAMBIZ ZAND
PRIMARY EXAMINER